

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

ROBERT BOWERS,

Defendant.

)
)
)
)
)
)
)
)
)
)

2:18-CR-00292-DWA

AMBROSE, United States Senior District Judge

MEMORANDUM OPINION AND ORDER OF COURT
RE: MOTION TO SUPPRESS NO. 12

Summary

The Defendant filed a Motion to Suppress Evidence Seized During Search and Seizure of Records and Information Associated with Domain Name (“onedingo.com”) from Internet Service Provider Tucows/Hover/eNom (“Tucows”) – Motion to Suppress No. 12. (ECF No. 299, sealed at No. 313). The Defendant’s Motion to Suppress is brought pursuant to Rule 12(b)(3)(C) of the Federal Rules of Criminal Procedure and the Fourth Amendment of the U.S. Constitution. *Id.* The Government filed a Response in Opposition thereto. (ECF Nos. 350, sealed at No. 360). The Defendant filed a Reply and the Government filed a Surreply. (ECF Nos. 381, sealed at No. 393 and 401). After careful consideration and for the reasons set forth below, Motion to Suppress No. 12 (ECF Nos. 299, sealed at No. 313) is denied.

Background

On November 6, 2018, the Government submitted an affidavit in support of an Application for a warrant to search and seize records from Tucows. (ECF No. 313-1, pp. 10-20). The warrant was issued on that same date. *Id.*, pp. 1-9. The affidavit described the investigation into the Defendant’s alleged conduct in the mass killing and wounding of others at the Tree of Life Synagogue (“Synagogue”). The application sought the authorization to search “information

associated with the domain name, ONEDINGO.COM, including,” *inter alia*, R.Bowers@onedingo.com, warroom@onedingo.com, iffy+gabai@onedingo.com, iffy+uscca@onedingo.com. *Id.* at pp. 3-4 (“Attachment A”). The particular things to be seized, set forth in Attachment B, were identified as “All information ...that constitutes the fruits, evidence and instrumentalities of violations” of the crimes charged involving the Defendant “since April 27, 2018, relating to the development, publishing, advertisement, access, use, administration or maintenance of any website, email server, and file storage enumerated in Attachment A...including [items] indicating hatred, bias, or prejudice based upon race and/or religion...” *Id.* at p. 5.

Analysis

Pursuant to the Fourth Amendment, the Defendant seeks to suppress evidence seized during the search and seizure from Tucows of information associated with the domain “onedingo.com” because the “warrant was overbroad in failing to limit the information seized to that for which there may have existed probable cause.” (ECF No. 299/313, p. 1). In opposition, the Government argues, *inter alia*, there was a substantial basis set forth in the Application for the warrant to establish probable cause. (ECF No. 350/360). The Government continues that even if there was a Fourth Amendment violation, the good faith exception to the exclusionary rule applies such that suppression is not warranted. *Id.* In Reply, the Defendant urges that probable cause is lacking and that the good faith doctrine does not apply. (ECF No. 381/393).¹

The Fourth Amendment prohibits “unreasonable searches and seizures” stating that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. Amend. IV. To that end, a warrant is overbroad when it permits the search and seizure of items for which there is no probable cause. *See, United States v. Yusuf*, 461 F.3d 374, 395 (3d Cir. 2006).

¹ The parties have touched on the issue of standing in their submissions. For argument’s sake, I am assuming the Defendant has standing, without deciding the issue.

Probable cause is a fluid concept that turns on the particular factual context at hand. *Illinois v. Gates*, 462 U.S. 213, 232 (1983). The existence of probable cause is to be assessed through "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before [the magistrate], there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. In other words, the inquiry rests on a common-sense, totality of the circumstances analysis; each piece of information in an affidavit is not assessed in isolation. See *id.*, 462 U.S. at 230-31; *United States v. Conley*, 4 F.3d 1200, 1205–06 (3d Cir. 1993). Accordingly, our Court of Appeals has cautioned against "'overly compartmentaliz[ing]' the determination of probable cause." *United States v. Yusuf*, 461 F.3d 374, 390 (3d Cir. 2006).

A reviewing court does not conduct a *de novo* determination of probable cause, but determines whether a "substantial basis" existed for the magistrate's finding of probable cause. *Gates*, 462 U.S. at 236; *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002). In making the determination of whether there was a substantial basis for finding probable cause, "the Court confines itself 'to the facts that were before the magistrate judge, i.e., the affidavit, and [does] not consider information from other portions of the record.'" *Hodge*, 246 F.3d at 305, *quoting Jones*, 994 F.2d at 1055; *Zimmerman*, 277 F.3d 426, 430, n.3 (3d Cir. 2002).

In this context, "[a] court 'is entitled to draw reasonable inferences about where evidence is likely to be kept, based on the nature of the evidence and the type of offense.'" *United States v. Hodge*, 246 F.3d 301, 305-06 (3d Cir. 2001), *quoting United States v. Whitner*, 219 F.3d 289, 296 (3d Cir. 2000); *United States v. Jones*, 994 F.3d 1051, 1056 (3d Cir. 1993). "The resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants." *Hodge*, 246 F.3d at 305, *quoting Jones*, 994 F.2d at 1057-58. A reviewing Court is to "give great deference to the magistrate judge's probable cause determination." *Id.* at 305; *Zimmerman*, 277 F.3d at 432. That said, it does not "mean that reviewing courts should rubber stamp a magistrate's conclusions." *Jones*, 994 F.2d at 1055.

Probable cause requires certain connections between the place to be searched, the suspected criminal activity, and the items to be seized. This connection or “nexus” is an expression of the requirement that probable cause exists to believe that evidence of an offense will be found at the place to be searched and can be made by inference. *See, United States v. Stearn*, 597 F.3d 540 (3d Cir. 2010); *Hodge*, 246 F.3d at 305-07; *see also, United States v. Tsarnaev*, 53 F. Supp. 3d 450, 462 (D. Mass. 2014). Thus, consistent with the applicable common-sense inquiry and as acknowledged by the Defendant, direct evidence linking the place to be searched with criminal activity is not required to establish probable cause to search. *United States v. Burton*, 288 F.3d 91, 103 (3d Cir. 2002); *Hodge*, 246 F.3d at 305; *Jones*, 994 F.2d at 1056.

As to this Motion, the Defendant concedes that the warrant affidavit establishes a connection between criminal activity and the “R.Bowers@onedingo.com” email address but argues that it fails to provide facts to establish probable cause for all other items associated with the onedingo.com domain name that the Government sought to seize. (ECF No. 299/313, p. 4). “[T]he breadth of items to be searched depends upon the particular factual context of each case and also the information available to the investigating agent that could limit the search at the time the warrant application is given to the magistrate.” *Yusuf*, 461 F.3d at 395. Upon review, I find the affidavit set forth facts connecting the Defendant to the onedingo.com domain name and the onedingo.com domain name to criminal activity sufficient to provide a substantial basis that items sought from Tucows would contain evidence of the charged offenses including motive, bias hatred, and prejudice related to race and/or religion.

For example, the Application states that on October 27, 2018, the Defendant drove to and entered the Synagogue armed with multiple weapons, including handguns and an assault-style rifle, where people were in attendance and engaged in religious services and worship. (ECF No.

313-1).² The Defendant shot and killed multiple individuals and wounded many others. *Id.* “During the course of his deadly assault..., [the Defendant] made audible statements indicating an animus toward people of the Jewish faith” commenting “they’re committing genocide to my people. I just want to kill Jews” and repeating “comments regarding genocide, his desire to kill Jewish people, and that Jewish people need to die.” *Id.*

The Affiant continued, “[e]arly indications of the investigation are that BOWERS engaged in planning and premeditation prior to executing the killings and injury associated with this crime. BOWERS utilized software to wipe data from his computer hard drives to prevent law enforcement access to the data and used software encryption to secure his phone.” (ECF No. 313-1, p. 13). The Affiant also determined through open source research that the Defendant “used electronic communications and social media as the means to espouse his views toward race and religion.” *Id.* During the investigation, relatives of the Defendant provided “R.Bowers@onedingo.com” as one of the email accounts that the Defendant used in communicating with them. *Id.* This email address was confirmed by one of the Defendant’s prior employers. *Id.* at pp. 13-14.

The Defendant’s mother, Barbara Bolt, told law enforcement that he communicated with her “frequently via text, phone call and email and ...that she became aware of BOWERS’ bias toward Jewish people approximately four (4) to six (6) months ago and did not think he was always biased.” *Id.* at 14. On October 25, 2018, the Defendant sent his mother a “video email” about the Six Day war and that he was trying get her to “agree with or approve of his bias towards Jewish people.” *Id.* She believed he thought Jews were behind the immigrant caravan. *Id.* The FBI also interviewed Raymond Bolt, husband of the Defendant’s mother, who provided that the Defendant “despised Jewish people and had begun feeling this way two (2) to three (3) years ago, or more recent than that” and that he would send his mother email videos about his views. *Id.*

² A shotgun was later found in the Defendant’s vehicle.

Open source information from May 10, 2000, found a second email account using the same domain, warroom@onedingo.com, attached to the website www.warroom.com “which hosted information concerning a conservative radio host’s talk show...[and] indicated that BOWERS was the show archiver and appeared to store sound files for past shows conducted by the conservative radio host for later access by the public. BOWERS solicited sponsors for server space using the ‘warroom@onedingo.com’ email address.” *Id.* at pp. 14-15.

Open source information for the domain name “onedingo.com” showed that it was registered with Tucows. *Id.* at 15. The Affiant explained that domain names must be registered to individuals and Tucows provided that “onedingo.com” was owned by the Defendant. *Id.* at p. 18.

24. On November 1, 2018, Tucows/Hover/eNom provided records pursuant to a court order issued under 18 U.S.C. §2703(d) that established that BOWERS was the owner of the internet domain “onedingo.com”. The information confirmed that the domain hosted email services including **R.Bowers@onedingo.com**. Email transaction logs demonstrate that this account communicated by email with persons at gunownersaamerica.com; usconcealedcarry.com; GAB AI; Underwood Ammo, and Sig Sauer. The email transaction logs show 695 email communications, either as sender or as recipient, between **R.Bowers@onedingo.com** and shabaray@gmail.com from October 23, 2016 through October 25, 2018, the date that Barbara Bolt mentioned for BOWERS’ last “video email” communication....Shabaray@gmail.com has been confirmed to be the email account of BOWERS’ mother...The records also record 254 events going back to November 12, 2011 such as: user logins, user edits of passwords, domain renewals, creation of a mailbox; and service reactivations. Tucows/Hover/eNom have preserved the content of the account for production pursuant to legal process. From the email transaction logs, affiant is aware that BOWERS also established a large number of additional email accounts using the “onedingo.com” domain.

Id. at 15-16 (emphasis in original). The Affiant then listed additional email accounts and set forth his belief that “it is reasonable to infer that BOWERS may have also used his domain and email accounts at Tucows/Hover/eNom to communicate his animus toward other races and religions.” *Id.* at 16.

The Affiant also provided information about web hosting companies like Tucows and the types of information they may maintain. *Id.* at pp. 16-19.

Magistrate judges “may give considerable weight to the conclusions of experienced law enforcement officers....” *United States v. Whitner*, 219 F.3d 289, 296 (3d Cir. 2000); *see also*, *Yusef*, 461 F.3d at 385 (Information received from other law enforcement officials during the course of an investigation is generally presumed to be reliable.). In this Application, the Affiant specifically and aptly set forth breadth of his knowledge, training, and experience and that claims in his affidavit were based on the same.

3. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since August 2007. During that time, I have worked on investigations involving drug trafficking, violent crime, and criminal cyber investigations. I have received training in computer crime investigations. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search and seizure warrants, and the identification and collection of computer-related evidence. I am currently assigned to the FBI Pittsburgh Division’s Western Pennsylvania Opiate Task force.

4. The facts in this affidavit come from my personal observation, my training and experience, and information obtained from other agents and witnesses. ...

(ECF No. 313-1, pp. 10-11). The Affiant also provided that his statements were based on open source information, investigations and witness interviews by law enforcement officers, and audible statements heard by a law enforcement officer. (ECF No. 313-1). There is no suggestion of unreliability as to these sources. As a result, I find the magistrate judge was permitted to rely on all of the assertions made by Affiant in the Application.

Considering all of this information, along with the rest of the information in the affidavit and given the circumstances of this mass shooting, the magistrate was permitted to make reasonable inferences and such decisions are entitled to deference. *See, Jones*, 994 F.2d at 1056 (A magistrate judge is permitted to make reasonable inferences in connection with statements made in an affidavit in support of an application for a warrant.). I agree with the Government that there is a substantial basis, as set forth in the affidavit, for a magistrate to infer therefrom that there was a fair probability that evidence of the charged crimes would be contained within the information associated with the “onedingo.com” accounts owned by the Defendant, e.g. communications with

like-minded individual or co-conspirator could be contained in the email traffic on “onedingo.com” indicating his bias or motive, as well as to evidence regarding the evolution of the Defendant’s animus, and his discussions and ability to acquire weaponry and ammunition allegedly used in the mass shooting in the Synagogue. The Defendant’s concession that the affidavit connects the “R.Bowers@onedingo.com” email account to racial animus (ECF No. 299/313, p. 4) bolsters the inference that other “onedingo.com” accounts would also contain evidence of racial animus. Contrary to the Defendant’s assertions otherwise, these are not “after the fact rationalizations” or unreasonable inferential leaps but rather provide a substantial basis for reasonable inferences the magistrate could make when reading the Application as a whole in a common-sense manner in the context of the mass shooting.

I further note that Attachment B limited the Government’s seizure to information and records related to the charged offenses and “which indicat[e] hatred, bias, or prejudice based upon race and/or religion, including...email accounts...which relate to communication about ammunition; firearms related paraphernalia; firearms purchase or use; social media accounts; indicia of residency; motive related to race and religion, including but not limited to writings, literature, communications, objects, and paraphernalia indicating hatred, bias, or prejudice based upon race and/or religion; evidence of preparation, reconnaissance or research of the Tree of Life or any other synagogues.” (ECF No. 313-1, pp. 6-7). Additionally, there were temporal and other qualitative specifications. *Id.* Reading the Application as a whole and using a common-sense, totality of the circumstances approach, I find there was a substantial basis for the magistrate to conclude that there was a probable cause that the information and records associated with the domain name “onedingo.com” from Tucows would uncover evidence of the charged offense. Consequently, I find the warrant was not overbroad and suppression is not warranted.

Finally, even if the Defendant’s overbreadth argument had merit, the good faith doctrine applies such that suppression of the evidence is not warranted. *Herring v. United States*, 555 U.S. 135, 137 (2009) (“[S]uppression is not an automatic consequence of a Fourth Amendment

violation.”). The goal of the exclusionary rule is to deter Fourth Amendment violations. *Id.* at 139-140; *see also, United States v. Werdene*, 883 F.3d 204, 215 (3d Cir. 2018). Exclusion is a “last resort, not our first impulse.” *Id.* at 140; *U.S. v. Caesar*, No. 19-3961, 2021 WL 2559471, at *6 (3d Cir. June 23, 2021)(“Exclusion is a ‘bitter pill’ swallowed only where it would result in a ‘substantial deterrent effect’ that outweighs its resulting costs, [*U.S. v.] Leon*, 486 U.S. [897] at 907 [1984].”). Accordingly, if officers acted with an “objectively reasonable good-faith belief that their conduct [was] lawful or when their conduct involve[d] only simple, isolated negligence,” there is no deterrent effect justifying exclusion of evidence. *United States v. Katzin*, 769 F.3d 163, 171 (3d Cir. 2013); *Caesar*, 2021 WL 2559471 at *6. Thus, “to trigger the exclusionary rule, law enforcement conduct must be ‘deliberate, reckless, or grossly negligent,’ or involve ‘recurring or systemic negligence.’” *Caesar*, 2021 WL 2559471 at *6, *quoting, Herring*, 555 US at 143-44. Therefore, the good faith inquiry rests on “‘the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal’ in light of ‘all of the circumstances.’” *United States v. Horton*, 863 F.3d 1041, 1051 (8th Cir. 2017), *quoting, Herring*, 555 U.S. at 145.

In this case, there is no suggestion of deliberate, reckless, or grossly negligent disregard of the Fourth Amendment. I find suppression would have no appreciable deterrent effect because a reasonable officer would not have known that the detailed and limiting list of items to be seized in the warrant was invalid despite the magistrate judge’s authorization. Moreover, contrary to the Defendant’s position, as set forth above, the allegations set forth in the Application were not “merely conclusory.” Consequently, even if there was a Fourth Amendment violation, I find the good faith exception to the exclusionary rule applies and suppression is not warranted.

Therefore, the Defendant’s Motion to Suppress Evidence Seized During Search and Seizure of Records and Information Associated with Domain Name from Internet Service Provider – Motion to Suppress No. 12 – shall be denied.

An appropriate order shall follow.³

³ In his Reply to the Government's Opposition, the Defendant seeks an evidentiary hearing. (ECF No. 381/393). Based on the discussion above, I find a hearing is not necessary.

